CYBERCRIME IN NIGERIA: ISSUES AND CHALLENGES

Emma Osuji[*]

Abstract

Information technology, especially the internet, has remained one of the most impressive scientific developments in the history of mankind. It has bonded personal relationships, facilitated trade and commerce across all levels, and made life easier. This welcoming benefit of internet advancement has also been identified as having its attendant problems, which include high growth rate of criminality known as cybercrime. This paper systematically investigates the challenges which inhibit the successful elimination of cybercrime in Nigeria. The paper emphasizes that weak enforcement mechanisms, a slow judicial process and the slow process of forensic analysis among others, contribute to the inadequacy of the fight against cybercrime. This paper puts forward recommendations for regulatory bodies which will bring about efficient and adequate prosecuting mechanism. This will ensure that this menace is minimized in Nigeria.

Key words: *Internet Technology, Cybercrime, Internet, Legal Framework.*

Introduction

Globally, digitalization and internet-based activities have grown, with Nigeria as no exception to the adaptation of the expansion.[1] As much as internet expansion in Nigeria has its advantages and disadvantages, the exponential rate of the usage of computers and the internet in numerous establishments has had a hugely beneficial influence,[2] on government, commerce, education and other spheres of activity relating to mankind. The alarming growth of the internet and its wide acceptance in society has led to an increase in security threats all over the world and in Nigeria too.

In Nigeria today, several internet-assisted crimes known as cybercrimes are committed daily in various forms, such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, spoofing, piracy and phishing[3] among others. It must be noted that cybercrime has become a threat to various institutions and internet users either through computers or mobile technology.

Hence, the rapid growth of computer technology carries with it the evolution of various crimes on the internet,[4] with Nigeria as no exception. Nigeria is the third most targeted country for cybercrime in Africa.[5] Between the first and second quarters of 2021 and now, there has been more than a 32 percent jump in Malware in Trojan horse attack in Nigeria.[6] By this, we mean that a Malware that misleads users of its true intent by disguising itself as a standard program is installed

[*] **Emma Osuji Esq (KSM) Ph.D Lecturer in Department of Public Law, Faculty of Law Imo State University Owerri.**

1 Anwana, E.J., Ogundale A.T., Olannde E.S., and Idem, U.J., "The Prosecution of Cybercrime in Nigeria: Challenges and Prospects. *researchgate.net/public*. Accessed 24/5/2023.

2 *Ibid*.

3 Omodunbi, B., Odiase, P.O., Olaniyian O., "Cybercrime in Nigeria: Analysis, Detection and Prevention" *researchgate.net/public*. Accessed 24/5/2023.

4 Okorie, C.K., and Mbachu S. C., Complexities, Issues and Challenges on Cybercrime in Nigeria (eds) Chukwumaeze, U.U. and Okorie C.K., Exellence at the Bench, Essays and Selected Judgments in Honour of Honourable Justice Bernadine Ngozi Ukoha, Administrative Judge, Owerri Judicial Division, Imo State Judiciary, 2019, 165.

5 The Guardian "How to Protect Yourself from Cybercrime in Nigeria" *guardian.ng/features /hc*. Accessed 24/5/2023.

6 *Ibid*.

to exploit security gaps unknown to the general public as well as access smart phone data before it becomes encrypted via other applications.

An application such as malware is used to perpetrate digital crime by anyone who actively seeks to exploit weaknesses in technology for illegal purposes.[7] This exploitation of weaknesses in technology which manifests in cybercrime, has done a lot of damage to individuals, government and the global community as a whole. It has become a major cause for concern worldwide including Nigeria, hence adequate mechanisms must be put in place to ensure that offenders of the said crime are properly prosecuted.

Conceptualization of Cybercrimes

Cybercrimes are transnational in nature.[8] Cybercrimes are crimes committed without the perpetrators being physically, present at the locus.[9] Cybercrimes are committed in the impalpable world of computer networks.[10] The Black's Law Dictionary describes cybercrime as cyber theft and defines it as the act of using an online computer service, such as one on the internet to steal someone's else property or to interfere with someone's else use and enjoyment of property.[11] It further cites examples of cyber theft as hacking into a bank account to wrongfully credit one's account and debit another and interfering with a copyright by wrongfully sending protected materials over the internet[12] among others.

Cybercrimes being technologically driven have continuously and ingeniously made it difficult for cybercrime investigators to find solutions to such cybercrime.[13] Crimes committed over the internet are very different in nature when compared to the physical world,[14] hence the difficulty in tracking offenders. Crimes relating to cyber space do not show any form of foot print, tangible traces or objects to track criminals down easily. They possess, huge amount of complications when it comes to investigations.[15]

Cybercrimes can basically be categorized into four parts, namely; against individuals, against property, against society and against organization.[16] Email spoofing is the act of sending email with false sender addresses, usually as a part of phishing attack designed to steal personal information or infect the computer with malware.[17] Cybercrime against individual also involves spamming which deals with the sending of multiple copies of unsolicited mails such as chain letters. Again cyber defamation is also an aspect of cybercrime against individuals, wherein someone publishes defamatory matters against a person through the email.[18] Cybercrimes against individuals involve spoofing. Spoofing as it pertains to cyber security is when someone or something pretends to be something else in an attempt to gain a victims confidence, get access to systems, steal data, steal money or spread malware. Spoofing attacks come in many forms including email spoofing, GPS spoofing, extension spoofing, Facial spoofing, caller ID spoofing, website and/or URL spoofing, among others.[19] Similarly, cyber stalking, which involves online

7 Bello, T., "Anatomy of Cybercrime in Nigeria: The Legal Chronicle *paoers.ssm.com*. Accessed 24/5/2023.
8 *Ibid*.
9 Welfinder, "Scope of Cyber Security" *www.wefinder24.com*. Accessed 24/5/.2023.
10 *Ibid*.
11 Gainer, B.A., Blacks Law Dictionary, West Group, St Paul Minn 1999, 392.
12 *Ibid*.
13 Weffinder, *op. cit.*
14 *Ibid*.
15 *Ibid*.
16 Mali, P., "Classification of Cybercrime" *www.lawyersdubindia.com*. Accessed 24/5/2023.
17 *https://www.malware.com/sppofing.* Accessed 24/5/2023.
18 *Ibid*.
19 *Supra*.

harassment where a person is subjected to a plethora of online message and emails which are intimidating in nature is another aspect of cybercrime against individuals.[20]

Another class of cybercrime is cybercrime against property.[21] Credit card fraud, intellectual property crimes, internet time theft which deals with stealing, destroying or misusing the source code are prevalent.[22] Cybercrimes can also be committed against an organization. This specie of cybercrime deals with unauthorized access to a computer network without the permission of the owner.[23] It can happen by way of deleting data or copying of confidential information. An organization's system can be contaminated for purposes of injecting a virus into it.

Cybercrime against society is another class of cybercrime that affects the society greatly.[24] In this instance, the cyber-criminal indulges in forgery of currency, revenue stamps, mark sheet, and also carries out cyber terrorism by using computers to intimidate or coerce people and carry out the activities of terrorism sentence could be restructured.[25] Web jacking as an aspect of cybercrime against society permits hackers to gain access and control over website of another, and even change the contacts of the website for fulfilling political objectives or for money. This is a three sentence paragraph and it is problematic. A paragraph is made up of at least 4 to 5 sentences; reflect this observation where necessary in this paper

It must be noted that the cyber space allow these attackers to easily carry out their activities and such intrusion can be made effortlessly with very little risk of apprehension.[26] The internet provides anonymity and safety for persons involved in Cyber offences. These perpetrators leave no traces of their actions and this makes it extremely difficult to trace them.[27]

Cybercrime has spread to such proportion that a formal categorization of the crime is no longer possible.[28] Every single day gives birth to a new kind of cybercrime, making every single effort to stop it almost a futile exercise.[29] Criminals have discovered that the internet can provide new opportunities and multiple benefits for illicit businesses.[30] These miscreants have employed the internet as a tool for not only fraud and theft among others but also drug trafficking and criminal organization rackets that are concerned with exploitation and disruption of the society[31] Cybercrime perpetrators are always one step ahead in the sense that they create technology or come up with techniques to perpetrate a particular crime, leaving law enforcement personnel with a puzzle to unravel the crime and bring the culprits to book.

---

20 *Supra.*
21 Panda Security, "Types of Cybercrime" *www.pandasecurity.com*. Accessed 24/5/2023.
22 *Ibid.*
23 *Ibid.*
24 *Ibid.*
25 Sulaman, S., and Yunog, Z., "Understanding Cyber Terrorism from Motivational Perspectives" *www.jstor.org*. Accessed 24/5/2023.
26 Chowbe, V.S., "Concept of Cyber-Crime, Nature and Scope" www.researchgate.net. Accessed 24/5/2023.
27 *Ibid.*
28 Admindeepak, Nature and Scope of Cybercrime" deepakmiglani.com. Accessed 25/5/2023.
29 *Ibid.*
30 *Ibid.*
31 *Ibid.*

Cybercrime in Nigeria

Cybercrime in Nigeria is an emerging trend that is rapidly growing in scope and frequency.[32] The revolution in information and communication technology has greatly promoted the trend and scope of cybercrime in Nigeria,[33] as the internet which is of course the greatest promoter of cybercrime.

In Nigeria, the rate at which the Nigeria cyber space is subjected to daily attacks from unscrupulous minds and criminal elements has continued to remain alarming.[34] Cybercrimes have taken a dangerous toll on individual businesses, institutions, government and the economy.[35] It has become one of the main avenues of getting rich quick.[36] According to Checkpoint, a global network cyber security vendor, Nigeria and Kenya recorded a massive rise in cybercrime in the first six months of 2022 with phishing and scams hitting 438 percent and 174 percent respectively.[37] The Economic and Financial Crimes Commission stated that in 2022, 2,800 persons were convicted of cybercrime in Nigeria.[38] The convicted persons, according to the commission were mostly youths. Hence, the youths have become cyber-creatures spending a significant amount of time online.[39] As the digital world expands, so does cybercrime in Nigeria.[40]

The rising cyber-attacks in Nigeria have caused more economic, social and cultural harm than good.[41] It is estimated that Nigeria loses over N500m yearly to cybercrime alone.[42] This accounts for 0.088 percent of the country's Gross Domestic Product.[43] These attacks on the cyber space range from those targeting business, to individuals and bank accounts, phones and computers as well. The funny thing is that these cyber criminals do not discriminate. They can affect very poor homes as well as rich ones. People are not well informed on this issue; hence they prey on any class of people, including the very intelligent ones.

It is very clear that the escalation of cybercrime cannot be curtailed adequately by local crime prevention agencies alone, hence the effects have continued internationally.[44] Apart from the social menace cybercrime has created in our economic system, it has succeeded in throwing a large number of fraudsters into the economic system of Nigeria.[45] Fraudulent activities and practices through cybercrime have made a lot of young people emergency millionaires, even billionaires in the Nigeria economic system.[46] This is of course injurious to the economic system because such funds acquired illegally are not used productively to promote the economy.

Indeed, this may be referred to as economic sabotage resulting from cybercrime. The situation has affected Nigeria's image. The image of Nigeria in this connection has been adjudged battered both internally and externally. Provide reference Though cybercrime is a global phenomenon, individual countries suffer the effects differently depending on what laws such country has in place

---

32 Oni, M.J., "Cybercrime in Nigeria: "The Implication in our Economy and Social Image" *www.acta-pac.org*. Accessed 25/5/2023.
33 *Ibid*.
34 Omodunbi, B., Odiase, P.O., Olamyan and Esan, A., *op. cit.*
35 *Ibid*.
36 *Ibid*.
37 *Ibid*.
38 EFCC, "Over 2,800 Persons Convicted of Cybercrime in 2022" *www.premiumtines.ng.com*. Accessed 25/5/2023.
39 OAL, Cybercrimes and Cyber Laws in Nigeria: *All you need to know.oal.law*. Accessed 26/5/2023.
40 *Ibid*.
41 Jaiyeola, T., "How Nigeria can curb Rising Cyberattackes" *www.punch.com*. Accessed 26/5/2023.
42 *Ibid*.
43 *Ibid*.
44 Oni, M.J., *op. cit.*
45 *Ibid*.
46 *Ibid*.

to address the situation as well as how effective their law and crime prevention agencies are able to curtail the menace.[47] Hence an appraisal of the cybercrime law of Nigeria.

An Appraisal of the Cybercrimes (Prohibition and Prevention) Act 2015

The Cybercrimes (Prohibition and Prevention) Act 2015 of Nigeria is the existing legal framework for combating cybercrime in Nigeria. It has a significant impact on cyber criminality in Nigeria. The said law has created a comprehensive legal, regulatory framework for the prevention, detection, prosecution and punishment of cyber criminals.

By way of an overview the Cybercrime Act 2015, contains 8 parts and *59 sections*. *Part I*[48] covers *2 sections*, which contains objectives and application.

Part II[49] which covers protection of critical National Information Infrastructure deals with designation of certain computer systems or networks as critical national information infrastructure and audit and inspection of critical national information infrastructure.

Part III[50] provides for Offences and Penalties, and deals with Offences against critical national information infrastructure, Unlawful access to computers, Registration of cybercafé, Unlawful interception of communications, Unauthorized modification of computer program or data, System interference, Misuse of devices, Computer related forgery, Computer related fraud, Identity theft and impersonation, Child pornography and related offences, Cyber stalking, Cybersquatting, Cyber terrorism, Racist and Xenophobic offences, Attempt, Conspiracy, aiding and abetting, and finally Corporate liability.[51]

Part IV[52] which deals with duties of service providers and provide for Records retention and Protection of data, Interception of electronic communication and Failure of service provider to perform certain duties while *Part V*[53] which provides for Administration and enforcement contains, Coordination and enforcement, Establishment of the Advisory Council and functions and Powers of the council.

Part VI[54] which covers Search, Arrest and Prosecution provides for powers to Conduct Search and Arrest, Powers to conduct investigation or Search without warrant, Obstruction and refusal to release information, Prosecution of offences, Order of forfeiture of assets and order for Payment of compensation or restitution.

Part VII[55] which deals with Jurisdiction and International cooperation provides for Jurisdiction, Extradition, Request for mutual assistance, Evidence of pursuant to a request, form of request, Expedited preservation of Computer data and Designation of contact point. Hence *Part VIII*[56] providing for miscellaneous deals with Directive, Regulations, Interpretations and Citation.

47 *Ibid*.
48 *Part I sections (1)* and *(2)* of the Cybercrime (Prohibition Prevention) Act 2015.
49 *Part II sections (3)* and *(4) ibid*.
50 *Part III sections (5)* and *(36) ibid*.
51 *Ibid*.
52 *Part IV sections (37)* and *(40) ibid*.
53 *Part V sections (41)* and *(44) ibid*.
54 *Part VI sections (45)* and *(49) ibid*.
55 *Part VII sections (50)* and *(56) ibid*.
56 *Part VIII sections (57)* and *(59) ibid*.

However, only the parts and sections critical to this paper shall be examined. For instance, *section 7* of the Cybercrime (Prohibition and Prevention) Act 2015 provides thus:

> 7(1) from the commencement of this Act, all operators of a cybercafé shall register as a business concern with computer professional Registration Council in addition to a business name registration with corporate Affairs Commission. Cybercafé shall maintain a register of users through a sign-in register. The register shall be made available to law enforcement personnel whenever needed.

From the foregoing provision of *section 7 (1)* of the Act, it is mandatory for every cybercafé operator in Nigeria to register its business with Computer Professional's Registration Council and the cybercafé operators have to maintain a register of users. These conditions imposed on cybercafé operators are unnecessarily burdensome and onerous.

In addition to the provision for Registration with the Computer Professional's Registration Council, cybercafé operators must pay the fees, not minding the scale of the said cybercafé. Moreso, registration of cybercafé is not within the mandate of the Computer Professional's Registration Council whose mandate is to provide a regulated and standard driven environment for Information Technology.[57]

The duty of the said Computer Professional's Registration Council is centered on Information Technology education and standards in computer. There is nothing to suggest that this organization is capable of containing this additional responsibility placed on her by the Act, hence the organization does not have the spread to deal with registration of cybercafé.

Again, *section 8* of the Act which provides for system interference is another aspect of the cybercrime Act considered to be controversial.

It provides thus:

> Any person who without lawful authority, intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of computer system by imputing, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or liable to pay a fine of not than N5,000,000 or to both fine and imprisonment.

In as much as this section is intended to protect the systems from unlawful interference, misuse or, a misinterpretation of this section, notably could lead to individuals being wrongfully prosecuted, hence innocent individuals who never intended to do any act that could hinder the functioning of a computer system could be punished. This is so suggested because, a virus in a computer system could lead to system interference and a person could be accused of that. Hence it is suggested that the language of this section of the Act be amended to provide a greater clarity about what truly constitutes system interference.

Again, the concept of system interference which has been vilified by the law as a form cyber stalking, could have a chilling effect on free speech. Given the broad and vague language used in

[57] See *section 2* of the Computer Professional's Council Act 1993.

the Act, individuals who expresses opinion that are critical of the government or other powerful entities may be targeted and accused of system interference.

Furthermore, misuse of the offence of system interference could result to infringement of privacy right. Law enforcement agencies may use the offence as a pretext to conduct surveillance on individuals or groups, hence violation of right to privacy[58] with its significant implications on rule of law, human rights and democratic governance.

Furthermore, *section 29 (2) (b)*[59] of the Cybercrime (Prohibition and Prevention) Act 2015 is considered to be another controversial aspect of this Act. It provides thus:

> Where a body corporate is convicted of an offence under this Act, the court may order that the body corporate shall therefore and without any further assurances, but for such order, be wound up and all its assets and properties forfeited to the federal government.

Indeed, this provision is heavy and high handed. One of the known principles of criminal law is that punishment should be commensurate to the offence committed.[60] In this regard the forfeiture of assets of the convicted corporate body to the Federal Government without regard to the creditors and shareholders of the said corporate body is to say the least unfair and definitely not encouraging to innocent investors, hence it is suggested that the law be amended to reflect a consideration on the side of innocent investors and creditors with a view to protecting their investment.

Another section of the Cybercrime (Prohibition and Prevention) Act 2015 which calls for examination is *section 48 (4)* which provides thus:

> Any person convicted of an offence under this Act shall have his international passport cancelled. In the case of a foreigner his passport shall be withheld and only returned to him after he has served the sentence or paid the fine imposed on him.[61]

This would appear to be a violation of the constitutional right to freedom of movement as provided for under the 1999 Constitution of Nigeria (as amended)[62] and as decided in the case of *Director of State Security services vs Olisa Agbakoba*.[63] It must be noted that the Passport (Miscellaneous Provision) Act gives the power to cancel a passport in just very few cases including where the passport has expired, where it was obtained by fraud, where a person unlawfully holds more than one passport and it is in the interest of the public to so do.[64]

However, under the Cybercrime (Prohibition and Prevention) Act, 2015 any cancellation of a passport on the basis of conviction would appear to be justified as being done for public interest. Since all the offences under the Act could lead to a cancellation of a passport, the absurdity would be that a minor offence as cybersquatting would lead to cancellation of passport on conviction. Again, it is submitted that this section and provision of the Act is not commensurate with the punishment. Moreso, the person whose passport was cancelled must have been sentenced or paid fine whichever way. This amounts to double jeopardy, hence it is suggested that the law be

---

58 *Section 37* of the 1999 Constitution of Federal Republic of Nigeria (as amended).

59 *Section 29 (2) (b)* of the Cybercrime (Prohibition and Prevention) Act 2015.

60 Hirsch, A.V., "Commensurability and Crime Prevention: Evaluating Formal Sentencing Structure and their rational" *https://scholawlycommon.law.northwesttern.edu/jck*. Accessed 30/5/2023.

61 *Section 48 (4)* of the Cybercrime (Prohibition and Prevention) Act 2015.

62 *Section 41* of the 1999 Constitution of Nigeria (as amended).

63 (1999) LPELR-SC 5/1995.

64 See *section 5 (1) (a) (b) (c) (d*) of Passport (Miscellaneous Provision) Act LFN 2004.

amended to be able to separate the punishments to be inflicted on minor offences and serious offence as contained in the Act.

In addition to above controversies surrounding the Act, it created several offences without adequate stipulation for the enforcement of its provisions. It would serve better to mention these offences [65] Again the Act failed to confer powers on any specific law enforcement agency to enforce the provision of the Act.

Furthermore, the Act attempts to regulate the activities of banks and financial institution in Nigeria, whereas such activities of the bank are already regulated by Banks and other Financial Institution Act.[66] Such duplication, it is suggested may create challenges for the court when faced with deciding which Act is applicable in a given situation.

Issues and Challenges

Issues

Despite the criticisms against the Cybercrime (Prohibition and Prevention) Act 2015, there are other issues and challenges identified. One of the notable issues confronting the success of combating cybercrime in Nigeria is lack of coordination among various security agencies. There is absolutely no coordination and meeting point for security agencies in Nigeria, where ideas are exchanged for purposes of reinforcement of capacities and ideas on how to combat cybercrime. Unlike in the United Kingdom, where cybercrime unit has brought together law enforcement agencies and experts into a single elite unit.[67] This has succeeded in providing access to specialist capabilities in combating cybercrime in the United Kingdom, hence Nigeria should emulate the same pattern to improve their capabilities in fighting cybercrime.

Similarly, under the South African jurisdiction, agencies and organizations come under an umbrella to provide the South African police service with expertise by way of collaboration.[68] A designated point of combat is established to facilitate exchange of ideas between agencies in combating cybercrime in South Africa.[69]

Furthermore the issue of jurisdiction has always been pointed at as an issue in fighting cybercrime. This is so because it is transnational in nature and transcends states and jurisdictions.[70] Where a cybercrime offender is domiciled in another country as well, it becomes a problem for the court to try such offender, as the court may be faced with jurisdictional issues, geographically. Hence extradition would readily come to mind.[71] In most cases extradition is seen as an option but there must a treaty in that regarded existing among the states involvement.[72]

Again, it is a fact that in criminal prosecution, the prosecution must prove his case beyond every reasonable doubt before a conviction can be secured. Thus, in prosecuting cybercrime offences, prosecution heavily relies on electronic evidence which is faced with the challenges of accessing

---

65 *Ibid*.
66 *Ibid*.
67 Home Office, Review of the Computer Misuse Act 1990 of the United Kingdom, *www.gov.uk*. Accessed 19/8/2023.
68 Ndaka, Y., CSIR Collaborates with South African Police Service to Strengthen Cybercrime Investigation. *www.news24.com*. Accessed 19/8/2023.
69 *Ibid*.
70 Okorie, C.K., and Mbachu, S.C., *supra*, 173.
71 *Ibid*.
72 *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-cost-ofcybercrime.pdf.* Accessed 19/8/2023.

electronic evidence resulting from lack of cooperation from service providers.[73] In Nigeria, there is no synergy among service providers and security agencies, this of course poses a great challenge in prosecution of cybercrime perpetrators.

Improper handling of electronic evidence is also another issue facing cybercrime prosecution in Nigeria. Some of the investigators of cybercrime offenders lack experience in handling of electronic evidence in compliance with admissibility rule and this may lead to the rejection of vital evidence in court.[74] For instance the Evidence Act, 2011why not engage with the current Evidence Act provides a guide on what a court should do in ascribing weight to a statement contained in a document produced by a computer.[75] The aforementioned section presupposes that the court in estimating the weight to be attached to a statement in a document produced by a computer, shall regard all the circumstances from which any inference can reasonably be drawn as to the accuracy, or otherwise of said statement.[76] Additionally, the court must give consideration as to whether or not the information reproduced from the computer was supplied or recorded contemporaneously with the existence of the facts dealt with in that information.[77] This is where experience in handling cybercrime investigation becomes expedient, because the weight that will be attached to such evidence by a court depends on how the evidence generated complies with the requirement of the evidence Act. Interestingly, the South Africa law[78] on the same issue of weight to be attached in evidence generated on cybercrime treats it same way as that of Evidence Act of Nigeria.

In addition to the above, is the unwillingness of witnesses to testify for the fear of either being killed or loose clientele banks, auto-mobile industries and insurance companies find it difficult to testify in cases of cybercrime for fear of loosing clientele among others.

Challenges

The major challenge which be-devils the adequate combat of cybercrimes is the deficiency in definition. This is so because the dynamic nature of the cybercrime related offences evolve as a result of the scope and development in computer world. Scholars argue that it is important to put in place a broad definition of the term i.e cybercrime, because of the diversity and rapid emergence of new technology in the society.[79]

Mention must be made of lack of infrastructure as posing a challenge to the fight against cybercrime in Nigeria. Improper monitoring of cybercrime perpetrators as a result of lack of sophisticated and modern gadgets has hampered the fight against cyber criminality in Nigeria.[80]

Furthermore, is the issue of the lack of a functional national database. An effective national database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records, as well trace their recent digital tracks could be rephrased.[81] Hence it is suggested that a functional database be created and made functional for purposes of checkmating cybercrime perpetrators.

---

73 Obuobisa, Y.A., Challenges faced Regarding Cybercrime and the Rule of Law in Cyber Space from the Performance of a Prosecutor in Ghana. *rm.coe.int….* Accessed 20/8/2023.

74 *Ibid*.

75 *Section 34 (1) (b)* of the Evidence Act 2011.

76 Alaba, O.A., Electronic Evidence with Cybercrime Act 2015, Jurist Publication Series, Lokoja 2019, 84.

77 *Ibid*.

78 See *section 15 (3)* of the Electronic Communication and Transaction Act, 25 of 2002 of South Africa.

79 Okorie, C.K., and Mbachu, S.C., *op. cit.*, 176.

80 Makeri, Y.A., "Cyber Security Issues in Nigeria and Challenges" *www.varcsse.com.* Accessed 20/8/2023.

81 *Ibid*.

It must be noted also that lack of standard and forensic National Central Control in the Cyber System has constituted a draw back in combating cybercrime malady.[82] There is no regulation of standards, no adequate computer security in place; all these put together frustrates the fight against cybercrime in Nigeria.

Despite the shortfalls, issues and challenges, the Act has done well in curbing the menace of cybercrime in Nigeria. For instance *section 23*[83] of the Act on child pornography and abuse is worth commending because the Act makes it an offence for anyone using computer system or network to engage a child in pornography or engage in sexual activities with a child who is below the age 18 years in a computer system or network.

It is suggested that this provision covers the use of the social media such as facebook, twitter, instagram as a tool for meeting minors, engaging in sexual activities with them and transmitting same through communication devices, as such devices would qualify as computer system under *section 58* of the Act.[84]

Conclusion

Nigeria is increasingly relying on the internet and other information technology tools to engage in personal communication and in conduct of business activities among other several benefits.[85] As much as these developments allow for enormous gains in productivity, efficiency and communication, it has loopholes which are capable of destroying an organization; hence the Cybercrime (Prohibition and Prevention) Act 2015 is put in place at least as the first legal framework to address the problems and loopholes arising from the use of internet and information technology in Nigeria.

The Act is commendable and requires proper implementation for purposes of it achieving the desired goals in checkmating cybercrime perpetrators who rely on information technology to perpetrate various crimes against individuals, corporate bodies and government agencies.

Recommendations

One of the issues observed in relation to *section 3* and 4 of the Act is the provision for protection of National International Infrastructure. In this regard the President of the Federal Republic of Nigeria acting on the recommendation of the National Security Adviser is by order empowered to publish in the Federal Gazatte and design some computer systems and networks as critical National International Infrastructure.[86] Sadly enough, there is no order published in the Federal Gazatte designating any computer system or network as Critical National International Infrastructure. Hence it is recommended that such be gazatted.

Again, there should be a definite law enforcement agency assigned with the execution of the provisions of the Act. This is so because no specific agency is saddled with the role of execution of the provisions of the Act especially in terms of prosecution.

---

82 Idem, U.J., Olarinde, E.S., Anwana E., and Ogundele, T.A., The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects *www.researchgate.net*. Accessed 20/8/2023.

83 *Section 23* of the Cybercrime (Prohibition and Prevention) Act 2015.

84 Onadeko, O.A., and Afolayan, A.F., "A Critical Appraisal of the Cybercrime Act, 2015 in Nigeria" *www.isrcl.com>2021/05*. Accessed 30/5/2023.

85 Omodunbi, B., Odiase, P.O., Olanyan, O., and Esan, A., *supra.*

86 *Section 3* and *4* of the Cybercrime (Prohibition and Prevention) Act 2015.